Advisory Alert

Alert Number: AAA20260108 **Date:** January 8, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that affect third-party components that's running within their VxRail Products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell VxRail Appliance - Versions 8.0.000 through 8.0.361
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000412375/dsa-2026-028-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-39806, CVE-2025-39843, CVE-2025-39883, CVE-2025-39925, CVE-2025-39981, CVE-2025-39982, CVE-2025-39983, CVE-2025-40300)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the Linux kernel of their products. These vulnerabilities could be exploited by malicious users to cause denial of service and privilege escalation. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:0271

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20026, CVE-2026-20027, CVE-2026-20029)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-20026**: This vulnerability exists because the Snort 3 detection engine improperly handles certain memory buffers when processing DCE/RPC traffic. An unauthenticated, remote attacker could exploit this by sending a specially crafted DCE/RPC request through an affected device. A successful exploit could allow the attacker to read the contents of the system memory, potentially exposing sensitive data. **CVE-2026-20027**: This vulnerability is caused by a logic error in how Snort 3 validates specific fields within a DCE/RPC packet. By sending a malformed DCE/RPC request, an unauthenticated, remote attacker could trigger an unexpected condition that causes the Snort process to crash and restart. This results in a temporary "Denial of Service" (DoS) condition where network traffic is either dropped or passes through without being inspected, depending on the device configuration. **CVE-2026-20029**: An XML External Entity (XXE) vulnerability located in the licensing component of the Cisco Identity Services Engine (ISE) web-based management interface. It occurs because the software's XML parser handles external entity references improperly when processing uploaded XML files. An authenticated attacker with administrative privileges could exploit this by uploading a malicious XML file. This would allow the attacker to bypass access controls and read arbitrary files from the underlying operating system of the ISE node. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	(If configured to use snort 3 releases prior to 3.5.0.0) Cisco Secure Firewall Threat Defense (FTD) Cisco IOS XE Software • 1000 Series Integrated Services Routers (ISRs) • 4000 Series ISRs • Catalyst 8000V Edge Software • Catalyst 8200 Series Edge Platforms • Catalyst 8300 Series Edge Platforms • Catalyst 8500L Edge Platforms • Cloud Services Routers 1000V • Integrated Services Virtual Routers Cisco Meraki MX Series • MX67, MX67C, MX67W • MX68, MX68CW, MX68W • MX75, MX84, MX85, MX95 • MX100, MX105, MX250, MX400, MX450, MX600 • MX Z4 and vMX (Virtual MX) (XXE Vulnerability) Cisco Identity Services Engine (ISE) / Cisco ISE Passive Identity Connector (ISE-PIC) • Versions prior to 3.2 • Versions prior to 3.2 patch 8 • Versions prior to 3.3 patch 8 • Versions prior to 3.4 patch 4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-dcerpc-vulns-J9HNF4tH • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-jWSbSDKt

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.